



FILED

JUL 18 2017

Clerk, U.S. District and  
Bankruptcy Courts

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH THE  
EMAIL ACCOUNT

[REDACTED]@GMAIL.COM

Case: 1:17-mj-00503  
Assigned To : Howell, Beryl A.  
Assign. Date : 7/18/2017  
Description: Search and Seizure Warrant

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION FOR A SEARCH WARRANT**

I, [REDACTED] being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with the email address provided for the Google Mail ("Gmail") Account [REDACTED]@gmail.com (hereinafter the "**Target Account**"), that is stored at premises owned, maintained, controlled, or operated by Google, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043 (hereinafter "Google"). The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Attachment A. Upon receipt of the information described in Attachment A, government-authorized persons will review that information to locate the items described in Attachment B.

[REDACTED]

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that MICHAEL DEAN COHEN has committed violations of 18 U.S.C. § 1014 (false statements to a financial institution), 18 U.S.C. § 1956 (money laundering), as well as 18 U.S.C. § 951 (acting as an unregistered foreign agent) and the Foreign Agents Registration Act (“FARA”), 22 U.S.C. § 611 *et seq.* There is also probable cause to search the information described in Attachment A for evidence, contraband, fruits, and/or instrumentalities of these crimes, further described in Attachment B.

#### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *Id.* §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States (including a magistrate judge of such a court) . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

#### **PROBABLE CAUSE**

6. As described below, the FBI is investigating COHEN in connection with, *inter alia*, statements he made to a known financial institution (hereinafter “Bank 1”) in the course of opening

a bank account held in the name of Essential Consultants, LLC and controlled by COHEN. The FBI is also investigating COHEN in connection with funds he received from entities controlled by foreign governments and/or foreign principals, and the activities he engaged in the United States on their behalf without properly disclosing such relationships to the United States government.

**A. Michael Cohen**

7. According to press reports and bank records collected during the investigation, COHEN served for over a decade as an executive in the Trump Organization, an international conglomerate with real estate and other holdings formerly controlled by President Donald Trump prior to his presidency. Until approximately January 2017, COHEN was reported to have held various positions within the Trump Organization. During an interview with *The Wall Street Journal* in or around January 2017, COHEN described his role as being “the fix-it guy . . . . Anything that [then-President-elect Trump] needs to be done, any issues that concern him, I handle.”<sup>1</sup>

8. In or around January 2017, COHEN made public statements that he would resign from the Trump Organization to serve as the personal attorney for President Trump (serving as an attorney to the President in his personal capacity, as opposed to as a member of the White House Counsel’s Office). COHEN recently has identified himself publicly—including on his personal Twitter account—as a personal attorney for the President.

9. As described in more detail below, on or about March 23, 2017, COHEN submitted paperwork to Bank 1, with whom he had a prior banking relationship and several existing accounts, for the purpose of opening a new account. In the section for customers to provide contact information, COHEN, by hand, struck out a previously provided e-mail address and in its place

---

<sup>1</sup> “Intelligence Dossier Puts Longtime Trump Fixer in Spotlight,” *Wall Street Journal*, Jan. 11, 2017.

wrote the Target Account as his current e-mail address.

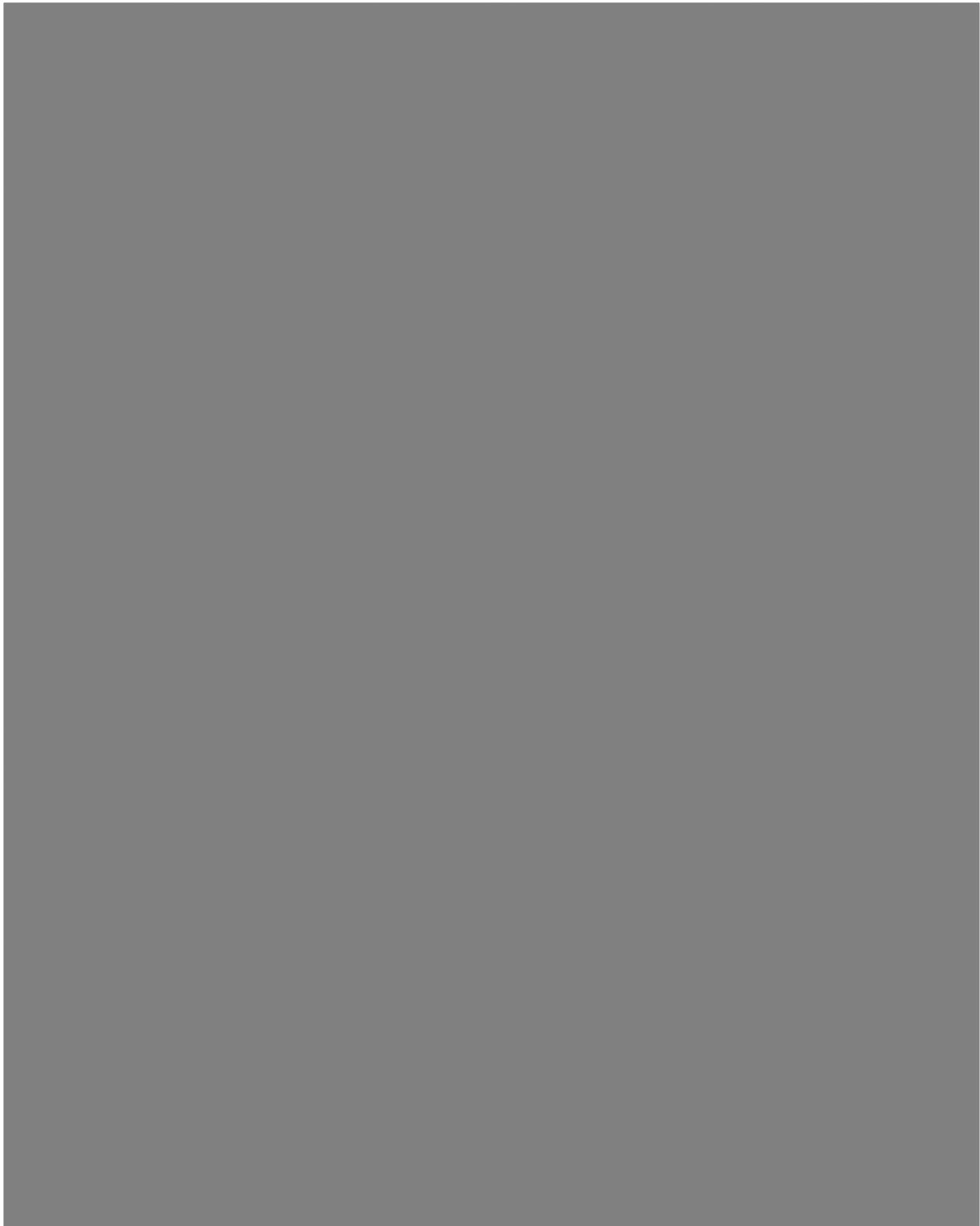
**B. Essential Consultants, LLC**

10. In or around June 2017, federal agents reviewed information supplied by Bank 1 based on activity that Bank 1 had observed from a number of accounts related to COHEN. According to information provided by Bank 1, COHEN has been a customer since approximately June 2011 and controls several checking and loan accounts, some in his personal name and others in the names of corporate entities. Agents have subsequently reviewed documents and records provided by Bank 1 related to COHEN and these various accounts.

11. According to information provided by Bank 1, on or about October 26, 2016, COHEN opened a new checking account in the name of Essential Consultants, LLC (“Essential Consultants”); COHEN was the only authorized signatory on the account. Corporate records show that Essential Consultants is a Delaware entity formed by COHEN on or about October 17, 2016.

12. According to Bank 1, when COHEN opened the Essential Consultants account, he represented during the course of Bank 1’s know your customer (“KYC”) procedures that he was opening Essential Consultants as a real estate consulting company to collect fees for investment consulting work. COHEN further represented that he intended to use his experience in real estate to consult on commercial and residential real estate deals, and that his typical clients were expected to be high net-worth domestic individuals. COHEN also represented that his purpose in setting up this account was to keep the revenue from his consulting—which he said was not his main source of income—separate from his personal finances.







**D. Foreign Transactions in the Essential Consultants Account with a Russian Nexus**

19. According to information provided by Bank 1, in or around October 2016, COHEN represented that he expected funds deposited into the Essential Consultants account would constitute income from COHEN's consulting work and that COHEN's consulting clients were expected to be domestic (that is, within the United States). COHEN also represented that he expected his clients to be U.S.-based, high-net worth individuals.

20. However, records from Bank 1 show substantial transactional activity that appears to be inconsistent with COHEN's KYC representations. Bank 1 records shows that the account received numerous deposits from foreign businesses and entities that do not reflect the stated client profile for the residential and commercial real-estate consulting services ostensibly being provided by Essential Consultants. Moreover, public records, media reports, and other publicly available sources indicate that some of these companies have significant ties to foreign governments or are entities controlled by foreign governments.

21. A search in or around July 2017 of the U.S. Department of Justice database of all agents currently or previously registered under the Foreign Agent Registration Act ("FARA") confirmed that neither COHEN nor Essential Consultants is or has been a registered agent of a foreign government.<sup>6</sup> All FARA registration is handled by the U.S. Department of Justice's National Security Division in Washington, D.C.

---

<sup>6</sup> The database is publicly available at <https://www.fara.gov/>.

i. Deposits by Columbus Nova, LLC

22. According to records obtained from Bank 1 through June 1, 2017, in the first five months of 2017, the Essential Consultants bank account received five deposits, each in the amount of \$83,333 (for a running total of \$416,665). The funds for all five deposits—four of which were wire transfers and one by check—came from an account at another bank held in the name of Columbus Nova, LLC.

23. Public records show that Columbus Nova, LLC is an investment management firm controlled by Renova Group (“Renova”), an industrial holding company based in Zurich, Switzerland. According to public news accounts, Renova is controlled by Viktor Vekselberg, a wealthy Russian national. Public news accounts also report that Vekselberg is an oligarch with various connections to Russian President Vladimir Putin and publicly met with Putin as recently as in or around March 2017.<sup>7</sup> According to the news articles, Vekselberg and Renova currently are involved in various infrastructure projects in Russia, such as the building of an airport in Rostov in advance of the 2018 FIFA World Cup, which is to be held in Russia. Vekselberg has been involved in various symbolic acts seen to be in the Russian national interest, such as the purchase and repatriation of historic Faberge eggs.<sup>8</sup>

ii. Plan to Lift Russian Sanctions

24. On or about February 19, 2017, *The New York Times* published an article reporting

---

<sup>7</sup> See, e.g., “Russia’s Putin Meets Tycoon Vekselberg,” *Reuters*, Mar. 14, 2017.

<sup>8</sup> On or about September 5, 2016, media outlets reported that Russian authorities arrested two of Vekselberg’s closest associates in connection with allegations that a subsidiary had paid over \$12 million in bribes to Russian government officials. Some media accounts speculated that the arrest of Vekselberg’s associates, as well as the commensurate searches of Renova’s head office, were intended as a warning from the Russian government that it wanted some form of cooperation or value from Vekselberg. See, e.g., “Another Billionaire Incurs Putin’s Wrath,” *Bloomberg*, Sept. 6, 2016.

that COHEN had been involved in distributing a proposed plan to the then-National Security Adviser, Michael T. Flynn, for the United States to lift sanctions on Russia as part of a negotiated end to the hostilities in Ukraine. The terms of the proposal appear to have been favorable to the Russians, according to *The New York Times* article.<sup>9</sup>

25. According to the article, prior to meeting with Flynn, COHEN had been approached by a Ukrainian politician (“Person 2”) and a Russian-American businessman (“Person 3”) who had prior business dealings with COHEN and the Trump Organization. According to the news report, Person 3 had previously been responsible for scouting deals in Russia for the Trump Organization through his company. According to the news reporting, COHEN met personally with both Person 2 and Person 3 about the proposal; during the meeting with Person 3, COHEN received the written plan in a sealed envelope.

26. According to *The New York Times*, COHEN has confirmed that he met with Person 2 and Person 3 and received the plan in a sealed envelope. In or around February 2017, COHEN then traveled to the White House and met the President in the Oval Office (the subject of the meeting is unclear). According to COHEN, during that trip, he left the proposal in the office occupied by then-National Security Adviser Flynn. According to *The New York Times*, COHEN stated that he was waiting for a response at the time that Flynn was forced from his post as the National Security Adviser.

27. The United States continues to investigate if any of the payments or financial relationships described above, or other relationships described further below, were connected to COHEN’s involvement in the distribution of a plan to lift Russian sanctions.

---

<sup>9</sup> “A Back-Channel Plan for Ukraine and Russia, Courtesy of Trump Associates,” *New York Times*, Feb. 19, 2017.

**E. Other Foreign Transactions in the Essential Consultants Account**

i. Deposits by Korea Aerospace Industries Ltd.

28. According to Bank 1, on or about May 10, 2017 and June 9, 2017, the Essential Consultants bank account received two deposits in the amount \$150,000 (totaling \$300,000 between the two deposits) from a bank account in Seoul, South Korea. According to documents obtained from Bank 1, the account holder from which the money was sent is Korea Aerospace Industries Ltd. (“KAI”). According to its public website, KAI is a South Korea-based company that produces and sells fixed-wing aircraft, helicopter aircraft, and satellites. Public news accounts report that KAI has partnered with Lockheed Martin to bid later this year on a \$16 billion U.S. Air Force T-X Trainer Jet Replacement Program.

29. According to publicly available materials and press accounts, as well as the company’s financial disclosures, the Republic of Korea (South Korea) government has significant ties to KAI. KAI itself was formed in 1999 as part of a government-led effort to consolidate South Korea’s aerospace industry manufacturers into a new single entity. KAI holds the exclusive rights for all of the government’s military logistics and aerospace projects.<sup>10</sup> The South Korean government, through the Korea Development Bank, is the largest shareholder in KAI and its largest debt holder.<sup>11</sup> According to information provided by Bank 1, messages related to the transfer of funds from KAI indicated that the purpose of these payments was “consulting services.”

ii. Wire Transfers from a Kazakhstani Bank

30. According to Bank 1, on or about May 22, 2017, the Essential Consultants bank

---

<sup>10</sup> See, e.g., Andrew Tylecote & Francesca Visintin, *Corporate Governance, Finance and the Technological Advantage of Nations* (2008), at 165–66; International Business Publications, *Korea South: A “Spy” Guide* (2016), at 229–31.

<sup>11</sup> KAI, Annual Report 2014, available at [https://www.koreaaero.com/upload\\_images/new\\_pdf/annual/PDF/Annual\\_report\\_eng\\_2014.pdf](https://www.koreaaero.com/upload_images/new_pdf/annual/PDF/Annual_report_eng_2014.pdf).

account at Bank 1 received a \$150,000 deposit from an account at Kazkommertsbank, a bank in Kazakhstan. According to Bank 1, the listed account holder at Kazkommertsbank was a second Kazakhstani bank named BTA Bank, AO. Bank 1 reported that a message accompanying the wire payment indicated that the agreement was a “monthly consulting fee as per Inv BTA-101 DD May 10, 2017 consulting agreement W/N DD 08 05 2017 CNTR W/NDD 08/05/2017.”

31. According to press reports, BTA Bank has been mired in a multi-billion dollar fraud that implicates its former top executives. According to a *Forbes* article published in or around February 2017, for example, BTA Bank’s auditors PricewaterhouseCoopers previously identified a \$10 billion discrepancy on the bank’s balance sheets.<sup>12</sup> Subsequent investigation by forensic accountants revealed that a unit of BTA had been used to issue billions of dollars’ worth of credit for property development and other deals in Russia, Ukraine, and Belarus. The investigation also indicated that funds illicitly had been removed from the bank through shell companies set up in the names of executives’ family members.

iii. Wire Transfers from Novartis Investments, SARL

32. Bank 1 also reported that on or about April 15, 2017 and May 15, 2017, the Essential Consultants account at Bank 1 received deposits in the amount of \$99,800 (totaling \$199,600) from a Swiss bank account held in the name of Novartis Investments, SARL. Novartis Investments, SARL is the in-house financial subsidiary of the Swiss pharmaceutical company Novartis AG.

**F. Bo and Abe Realty, LLC**



---

<sup>12</sup> “How To Get Back A Lost \$10B: One Bank’s Tale in Europe’s Biggest Alleged Fraud,” *Forbes*, Feb. 6, 2017.



Records show that the ultimate source of funds used to repay the HELOC funds came from a different company associated with COHEN, operating under the name Bo and Abe Realty, LLC (“Bo and Abe Realty”).

35. According to records of incorporation obtained from the New York Department of State, Division of Corporations, Bo and Abe Realty LLC was incorporated on or about July 29, 2013. Documents show that the organizer was Michael Cohen and the associated business address was COHEN’s residential address at 502 Park Avenue, [REDACTED] New York, NY 10022. No other agents or addresses were listed on the incorporating paperwork.

36. On or about July 31, 2013, Bank 1 records show that COHEN signed account opening documentation in order to open a bank account in the name of Bo and Abe Realty. In the documentation, COHEN identified himself as the President of Bo and Abe Realty; the opening documentation described the purpose of the business as the “purchase of real estate.” The account opening documentation also listed two other signatories on the account: COHEN’s brother (“Person 4”), and Person 4’s mother-in-law (“Person 5”). Both Person 4 and Person 5 were identified as



“members” of the company.<sup>14</sup>

**G. Use of the Target Account**



39. On or about March 21, 2017, an employee from Bank 1 sent an email to an email address associated with the Trump Organization that had in the past been used by COHEN. Bank records obtained from Bank 1 show that the employee received an automatic reply from the email address with the following message: “Effective January 20, 2017, I have accepted the role as personal counsel to President Donald J. Trump. All future emails should be directed to

---

<sup>14</sup> A sizeable portion of the funds deposited into the Bo and Abe Realty account came from an account in Person 5’s name. A review of documents provided by Bank 1 as well as information provided by other financial institutions indicate that both Person 4 and Person 5 are involved in and receive significant funds through a different entity operating under the name Ukrethanol, LLC (“Ukrethanol”). Ukrethanol has been involved in a series of suspicious transactions and has been suspected of possible money laundering or structuring. For example, in or around June 2013, Bank 3 closed a business account held in the name of Ukrethanol and exited its relationship with the company as a result of suspicious activity in the business account. The government continues to investigate the source of the Ukrethanol funds and the ultimate disposition of these monies.

mdcohen212@gmail.com [the **Target Account**] and all future calls should be directed should be directed to 646-853-011.”

40. On or about March 23, 2017, COHEN submitted new paperwork to Bank 1 in order to open another account (this one in the name of a newly incorporated entity with the name “Michael D. Cohen & Associates P.C.”). In the section for customers to provide contact information, COHEN by hand struck out a previously provided e-mail address affiliated with the Trump Organization. In its place, COHEN wrote the Target Account as his e-mail address for contact purposes.

41. On or about April 6, 2017, COHEN, using the **Target Account**, emailed an employee at Bank 1 about a pending wire to the Essential Consultants account. COHEN attached images of another conversation with another person who asked COHEN to confirm the routing numbers to his bank account.

#### **BACKGROUND CONCERNING GOOGLE MAIL**

42. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail (“email”) access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the Target Account. Subscribers obtain an account by registering with Google Mail. During the registration process, Google Mail asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google Mail subscribers and information concerning subscribers and their use of Google Mail services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence

of the crimes under investigation because the information can be used to identify the account's user or users.

43. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

44. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

45. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

46. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.<sup>15</sup>

47. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct

---

<sup>15</sup> It is possible that Google stores some portion of the information sought outside of the United States. In *Microsoft Corp. v. United States*, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information—including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of Google. The government also seeks the disclosure of the physical location or locations where the information is stored.

under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

**PRESERVATION OF THE TARGET ACCOUNT**

48. On or about June 21, 2017, the Federal Bureau of Investigation sent a request, pursuant to 18 U.S.C. § 2703(f), to Google, requesting that Google preserve all content associated with the Target Account.

**FILTER REVIEW PROCEDURES**

49. Review of the items described in Attachment A and Attachment B will be conducted pursuant to established procedures designed to collect evidence in a manner consistent with professional responsibility requirements concerning the maintenance of attorney-client and other operative privileges. The procedures include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privileges.

*[Remainder of this page left intentionally blank]*

**CONCLUSION**

50. Based on the forgoing, I request that the Court issue the proposed search warrant.

**REQUEST FOR SEALING**

51. I further request that the Court order that all papers in support of this application, including the application, affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

[Redacted]  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on this 18<sup>th</sup> day of July, 2017.

Beryl A. Howell  
The Honorable Beryl A. Howell  
Chief United States District Judge

**ATTACHMENT A**

This warrant applies to information associated with the Google Mail Account

[REDACTED] @gmail.com that is stored at premises owned, maintained, controlled, or operated by  
Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

**ATTACHMENT B**

**I. Information to be disclosed by Google**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Google (hereinafter "the Provider"), regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that have been deleted but are still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided

during registration, all other user names associated with the account, all account names associated with the subscriber, methods of connecting;

- f. All search history or web history;
- g. All records indicating the services available to subscribers of the accounts;
- h. All usernames associated with or sharing a login IP address or browser cookie with the accounts;
- i. All cookies, including third-party cookies, associated with the user;
- j. All records that are associated with the machine cookies associated with the user; and
- k. All telephone or instrument numbers associated with the Account (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”).

## **II. Information to be Seized by the Government**

All information described above in Section I that constitutes evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1014 (false statements to a financial institution) and 18 U.S.C. § 1956 (money laundering), as well as 18 U.S.C. § 951 (acting as an unregistered foreign agent) and the Foreign Agents Registration Act (“FARA”), 22 U.S.C. § 611 *et seq.*, involving Michael Dean Cohen and occurring on or after January 1, 2016, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Communications, records, documents, and other files involving Essential Consultants, LLC;
- b. Communications, records, documents, and other files involving Bo and Abe Realty, LLC;
- c. Communications, records, documents, and other files that false representations to a financial institution with relation to intended the purpose of an account or loan at that financial institution; the nature of any business or entity associated with an

account a financial institution; the source of funds flowing into an account; or the purpose or nature of any financial transactions involving that financial institution;

- d. Records of any funds or benefits received by or offered to Michael Dean Cohen by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
- e. Communications, records, documents, and other files that reveal efforts by Michael Dean Cohen to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
- f. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;
- g. Evidence indicating the account owner's state of mind as it relates to the crimes under investigation;
- h. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and
- i. The identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with the account about any matters relating to activities conducted by Michael Dean Cohen on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
BUSINESS RECORDS PURSUANT TO FEDERAL RULE  
OF EVIDENCE 902(11)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, and my official title is \_\_\_\_\_. I am a custodian of records for Google. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google and that I am the custodian of the attached records consisting of \_\_\_\_\_ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google; and
- c. such records were made by Google as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

---

Date

---

Signature

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH THE  
EMAIL ACCOUNT  
[REDACTED]@GMAIL.COM

Case: 1:17-mj-00503  
Assigned To : Howell, Beryl A.  
Assign. Date : 7/18/2017  
Description: Search and Seizure Warrant

MOTION TO SEAL WARRANT AND RELATED DOCUMENTS AND  
TO REQUIRE NON-DISCLOSURE UNDER 18 U.S.C. § 2705(b)

The United States of America, moving by and through its undersigned counsel, respectfully moves the Court for an Order placing the above-captioned warrant and the application and affidavit in support thereof (collectively herein the "Warrant") under seal, and precluding the provider from notifying any person of the Warrant pursuant to 18 U.S.C. § 2705(b). In regard to the non-disclosure, the proposed Order would direct Google, an electronic communication and/or remote computing services provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043, not to notify any other person (except attorneys for Google for the purpose of receiving legal advice) of the existence or content of the Warrant for a period of one year or until further order of the Court.

JURISDICTION AND LEGAL BACKGROUND

1. The Court has the inherent power to seal court filings when appropriate, including the Warrant. *United States v. Hubbard*, 650 F.2d 293, 315-16 (D.C. Cir. 1980) (citing *Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 598 (1978)). The Court may also seal the Warrant to prevent serious jeopardy to an ongoing criminal investigation when, as in the present case, such jeopardy creates a compelling governmental interest in preserving the confidentiality of the Warrant. See *Washington Post v. Robinson*, 935 F.2d 282, 287-89 (D.C. Cir. 1991).

2. In addition, this Court has jurisdiction to issue the requested order because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is a “district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). As discussed fully below, acts or omissions in furtherance of the offense under investigation occurred within Washington, D.C. *See* 18 U.S.C. § 3237.

3. Further, the Court has authority to require non-disclosure of the Warrant under 18 U.S.C. § 2705(b). Google provides an “electronic communications service,” as defined in 18 U.S.C. § 2510(15), and/or “remote computing service,” as defined in 18 U.S.C. § 2711(2). The Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701-2712, governs how Google may be compelled to supply communications and other records using a subpoena, court order, or search warrant. Specifically, Section 2703(c)(2) authorizes the Government to obtain certain basic “subscriber information” using a subpoena, Section 2703(d) allows the Government to obtain other “non-content” information using a court order, and Section 2703(a)-(b)(1)(A) allows the Government to obtain contents of communications using a search warrant. *See* 18 U.S.C. § 2703.

4. The SCA does not set forth any obligation for providers to notify subscribers about subpoenas, court orders, or search warrants under Section 2703. However, many have voluntarily adopted policies of notifying subscribers about such legal requests. Accordingly, when necessary, Section 2705(b) of the SCA enables the Government to obtain a court order to preclude such notification. In relevant part, Section 2705(b) provides as follows:<sup>1</sup>

(b) Preclusion of notice to subject of governmental access. — A governmental entity acting under section 2703 . . . may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court

---

<sup>1</sup> Section 2705(b) contains additional requirements for legal process obtained pursuant to 18 U.S.C. § 2703(b)(1)(B), but the Government does not seek to use the proposed Order for any legal process under that provision.

deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

- (1) endangering the life or physical safety of an individual;
- (2) flight from prosecution;
- (3) destruction of or tampering with evidence;
- (4) intimidation of potential witnesses; or
- (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 U.S.C. § 2705(b). The United States District Court for the District of Columbia has made clear that a nondisclosure order under Section 2705(b) must be issued once the Government makes the requisite showing about potential consequences of notification:

The explicit terms of section 2705(b) make clear that if a courts [*sic*] finds that there is reason to believe that notifying the customer or subscriber of the court order or subpoena may lead to one of the deleterious outcomes listed under § 2705(b), the court must enter an order commanding a service provider to delay notice to a customer for a period of time that the court determines is appropriate. Once the government makes the required showing under § 2705(b), the court is required to issue the non-disclosure order.

*In re Application for Order of Nondisclosure Pursuant to 18 U.S.C. § 2705(b) for Grand Jury Subpoena #GJ2014031422765*, 41 F. Supp. 3d 1, 5 (D.D.C. 2014).

5. Accordingly, this motion to seal sets forth facts showing reasonable grounds to command Google not to notify any other person (except attorneys for Google for the purpose of receiving legal advice) of the existence of the Subpoena for a period of one year or until further order of the Court.

#### FACTS SUPPORTING SEALING AND NON-DISCLOSURE

6. At the present time, law enforcement officers of the FBI are conducting an investigation into violations related to 18 U.S.C. § 1014 (false statements to a financial institution), 18 U.S.C. § 1956 (money laundering), as well as 18 U.S.C. § 951 (acting as an unregistered foreign agent) and the Foreign Agents Registration Act (“FARA”), 22 U.S.C. § 611 et seq. arising out of

the conduct of Michael D. Cohen. It does not appear that Cohen is currently aware of the nature and scope of the ongoing FBI investigation into him.

REQUEST FOR SEALING AND NON-DISCLOSURE

7. In this matter, the government requests that the Warrant be sealed until further order of the Court and that Google and its employees be directed not to notify any other person of the existence or content of the Warrant (except attorneys for Google for the purpose of receiving legal advice) for a period of one year or until further order of the Court. Such an order is appropriate because the Warrant relates to an ongoing criminal investigation, the full scope of which is neither public nor known to the targets of the investigation, and its disclosure may alert these targets to the ongoing investigation and its scope. Once alerted to this investigation, potential targets would be immediately prompted to destroy or conceal incriminating evidence, alter their operational tactics to avoid future detection, and otherwise take steps to undermine the investigation and avoid future prosecution. In particular, given that they are known to use electronic communication and remote computing services, the potential target could quickly and easily destroy or encrypt digital evidence relating to their criminal activity.

8. Given the complex and sensitive nature of the criminal activity under investigation, and also given that the criminal scheme may be ongoing, the Government anticipates that this confidential investigation will continue for the next year or longer. However, should circumstances change such that court-ordered nondisclosure under Section 2705(b) becomes no longer needed, the Government will notify the Court and seek appropriate relief.

9. There is, therefore, reason to believe that notification of the existence of the Warrant will seriously jeopardize the investigation, including by giving the targets an opportunity to flee from prosecution, destroy or tamper with evidence, and intimidate witnesses. *See* 18 U.S.C.

§ 2705(b)(2)-(5). Because of such potential jeopardy to the investigation, there also exists a compelling governmental interest in confidentiality to justify the government's sealing request. *See Robinson*, 935 F.2d at 287-89.

10. Based on prior dealings with Google the United States is aware that, absent a court order under Section 2705(b) commanding Google not to notify anyone about a legal request, it is Google's policy and practice, upon receipt of a warrant seeking the contents of electronically stored wire or electronic communications for a certain account, to notify the subscriber or customer of the existence of the warrant prior to producing the material sought.

WHEREFORE, for all the foregoing reasons, the government respectfully requests that the above-captioned warrant, the application and affidavit in support thereof, and all attachments thereto and other related materials be placed under seal, and furthermore, that the Court command Google not to notify any other person of the existence or contents of the above-captioned warrant (except attorneys for Google for the purpose of receiving legal advice) for a period of one year or until further order of the Court.

Respectfully submitted,

ROBERT S. MUELLER, III  
Special Counsel

Dated: 7/18/2017

FILED

JUL 21 2017

Clerk, U.S. District and  
Bankruptcy Courts

## UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)INFORMATION ASSOCIATED WITH THE EMAIL  
ACCOUNT [REDACTED] @GMAIL.COM

Case: 1:17-mj-00503

Assigned To: Howell, Beryl A.

Assign. Date: 7/18/2017

Description: Search and Seizure Warrant

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the Northern District of California  
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

**YOU ARE COMMANDED** to execute this warrant on or before August 1, 2017 (not to exceed 14 days)  
 in the daytime 6:00 a.m. to 10:00 p.m.  at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to Hon. Beryl A. Howell  
(United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)

for \_\_\_\_\_ days (not to exceed 30)  until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued:

July 18, 2017 4:30 PM

Beryl A. Howell

Judge's signature

City and state:

Washington, DC

Hon. Beryl A. Howell, Chief U.S. District Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

<b>Return</b>		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
17-mj-00503	7/18/2017 8:18 pm	Google Legal Investigators Support
Inventory made in the presence of:		
Inventory of the property taken and name of any person(s) seized: Digital Files: Letter 1150069 1150069-20170719-1 See Attachment A for list of Hash values for Production Files		
<b>FILED</b> <b>JUL 21 2017</b> <b>Clerk, U.S. District and</b> <b>Bankruptcy Courts</b>		
<b>Certification</b>		
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.		
Date:	7/20/2017 	
<i>Printed name and title</i>		

**Attachment A: Hash Values for Production Files (Google Ref. No. 1150069)**

mdcohen212.AccountInfo.Preserved.txt:

MD5- 50f6db8a1be9c101be73f72a1c759357  
SHA512-  
06266a86e331c847563d8ee7f055498992aaebf77ebd0ebb10ff1bc47b8e0a77787f95f2411814b  
5f8  
df27279bb190ec57fc350fcda79d98bfda66f049dc0e8b8

mdcohen212.AccountInfo.txt:

MD5- d79e32476bdd76d96e4627ef33491afd  
SHA512-  
66c153872629c3e74363176de4053bf1c03f5ab4cc24d44678c079e830896b448f6f5f4c4c53926  
df  
db1386c5cdadfe0558c4b1d87c9767d711fdda856ecc02b

mdcohen212.Calendar.Events.zip:

MD5- 5c61a4e43e73f026898d8a5ff8b0eea1  
SHA512-  
4ff150b49cd4918edd4ee04e9849b81575391306e46a74032d58b0d9d98e5f05b951c4947b6e62  
b4  
be08aed73a90438d3991ed8d349ddb8ca42e862eb42a89ba

mdcohen212.Drive.Metadata.zip:

MD5- 431db7ff8fe7e2ae571f8cc5f40c7273  
SHA512-  
0da895a52d31a294a643dab76fbb3817750293f445d366976f3889224942dee55f52067350a1a8  
4c6  
893afb548808494728818e5841545a53117a45c416b9ae8

mdcohen212.Drive\_001.zip:

MD5- 09d55ffe8a5703671faf1671de9865c9  
SHA512-  
c89b7a84be5342774d53879b4a1d4f6ae1cf9805184024bc8b12905e740262aa5146ffd549ee82f  
fb7  
4e3fa257fe7ec23e600f9b66acc8268b6ff8f48718f99c

mdcohen212.Gmail.Contacts.vcf:

MD5- a5d644bde145431dd9599e20f2e711d1  
SHA512-  
df18fea2c08a3e9f675f6ab7f40115c118f049ba6b7adfc0884d6385158714a5e4c963ef8c902abe3  
57  
3141dc8a4aa83853b4d6476c87ea7ee8fb8532e690d59

mdcohen212.Photos.Albums.Preserved.zip:

MD5- 76cdb2bad9582d23c1f6f4d868218d6c  
SHA512-  
5e2f959f36b66df0580a94f384c5fc1ceeeec4b2a3925f062d7b68f21758b86581ac2adcfdde73a171  
a2  
8496e758ef1b23ca4951c05455cdae9357cc3b5a5825f

mdcohen212.Photos.Albums.zip:

MD5- 76cdb2bad9582d23c1f6f4d868218d6c  
SHA512-  
5e2f959f36b66df0580a94f384c5fc1ceeeec4b2a3925f062d7b68f21758b86581ac2adcfdde73a171  
a2  
8496e758ef1b23ca4951c05455cdae9357cc3b5a5825f

mdcohen212.Photos.Preserved.zip:

MD5- b6c4aab13458f28808ddd25737692169  
SHA512-  
06d260f45eef71eb42a8dc425c0f019ae01d8df3bc665fc6cb63083feec849d5583b154818fc6b94  
cf0  
b2dcc57f1a66157c8148d5958e78250ae252da72de1a2

mdcohen212.Photos.zip:

MD5- ab04ce1cdc0eb330153241e465828710  
SHA512-  
014b1f138ee97e671dd5486be69344b86ab1d7e760102adbf95dc13fb27a257b669c02fa91ed77  
0a5  
3fb2428f92aa19a07bfb15009ae20db004e997c6e8183b

mdcohen212.Search.txt:

MD5- cb2ae11777b8b1f2f30493ace25f74af  
SHA512-  
45a51b37e87e89ad7d01dd57470f994f8b6f245e4ae2c187008fb1188d9d2c36dda8363336ae35  
c0d  
8e62c814079356169835fb31c9040f021dc51765caab440

mdcohen212@gmail.com.Gmail.Content.Preserved.mbox:

MD5- e64225338cc0303f256d7b86c3dac70f  
SHA512-  
f0005c8ddc28a9d0ffb54039060e3e3735e0436532771ddaf86d3c7b56d85b75105d3b1580c792  
05e  
2a0f7233aa9de79d3789b6966f9777766743a6a94221cc4

mdcohen212@gmail.com.Gmail.Content.mbox:

MD5- 5658e05cee7ccfa3a7fbf7110755e0a2

SHA512-

d195fbf672310e43e47fede6dc0271c8bbbc8cccbde14e9faa7f4f3baacddca8250c516f06747be0  
851660308903ae5781bc817f0d3386da862fd57c0867c19f

**ATTACHMENT A**

This warrant applies to information associated with the Google Mail Account  
[REDACTED]@gmail.com that is stored at premises owned, maintained, controlled, or operated by  
Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

**ATTACHMENT B**

**I. Information to be disclosed by Google**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Google (hereinafter “the Provider”), regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that have been deleted but are still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided

during registration, all other user names associated with the account, all account names associated with the subscriber, methods of connecting;

- f. All search history or web history;
- g. All records indicating the services available to subscribers of the accounts;
- h. All usernames associated with or sharing a login IP address or browser cookie with the accounts;
- i. All cookies, including third-party cookies, associated with the user;
- j. All records that are associated with the machine cookies associated with the user; and
- k. All telephone or instrument numbers associated with the Account (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”).

## II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1014 (false statements to a financial institution) and 18 U.S.C. § 1956 (money laundering), as well as 18 U.S.C. § 951 (acting as an unregistered foreign agent) and the Foreign Agents Registration Act (“FARA”), 22 U.S.C. § 611 *et seq.*, involving Michael Dean Cohen and occurring on or after January 1, 2016, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Communications, records, documents, and other files involving Essential Consultants, LLC;
- b. Communications, records, documents, and other files involving Bo and Abe Realty, LLC;
- c. Communications, records, documents, and other files that false representations to a financial institution with relation to intended the purpose of an account or loan at that financial institution; the nature of any business or entity associated with an

account a financial institution; the source of funds flowing into an account; or the purpose or nature of any financial transactions involving that financial institution;

- d. Records of any funds or benefits received by or offered to Michael Dean Cohen by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
- e. Communications, records, documents, and other files that reveal efforts by Michael Dean Cohen to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
- f. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;
- g. Evidence indicating the account owner's state of mind as it relates to the crimes under investigation;
- h. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and
- i. The identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with the account about any matters relating to activities conducted by Michael Dean Cohen on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals.